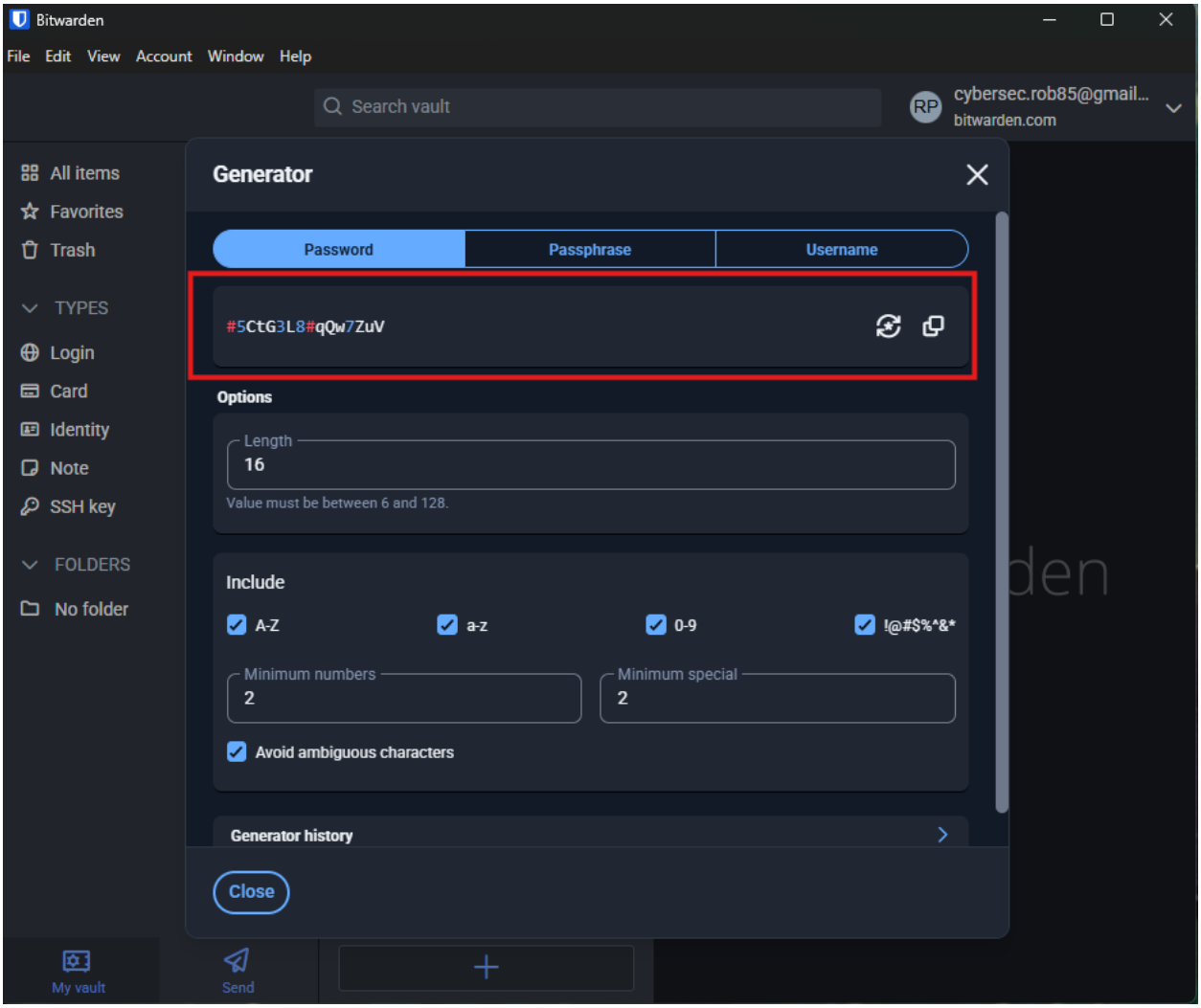
Lab Assignment 1 – User Security

Task 1: Download and install a password manager. There are many that are available. Please do some research on industry accepted options and see which one you would prefer to use.

Deliverable: None for Task 1

Task 2: Generate a strong password using selected Password Manager

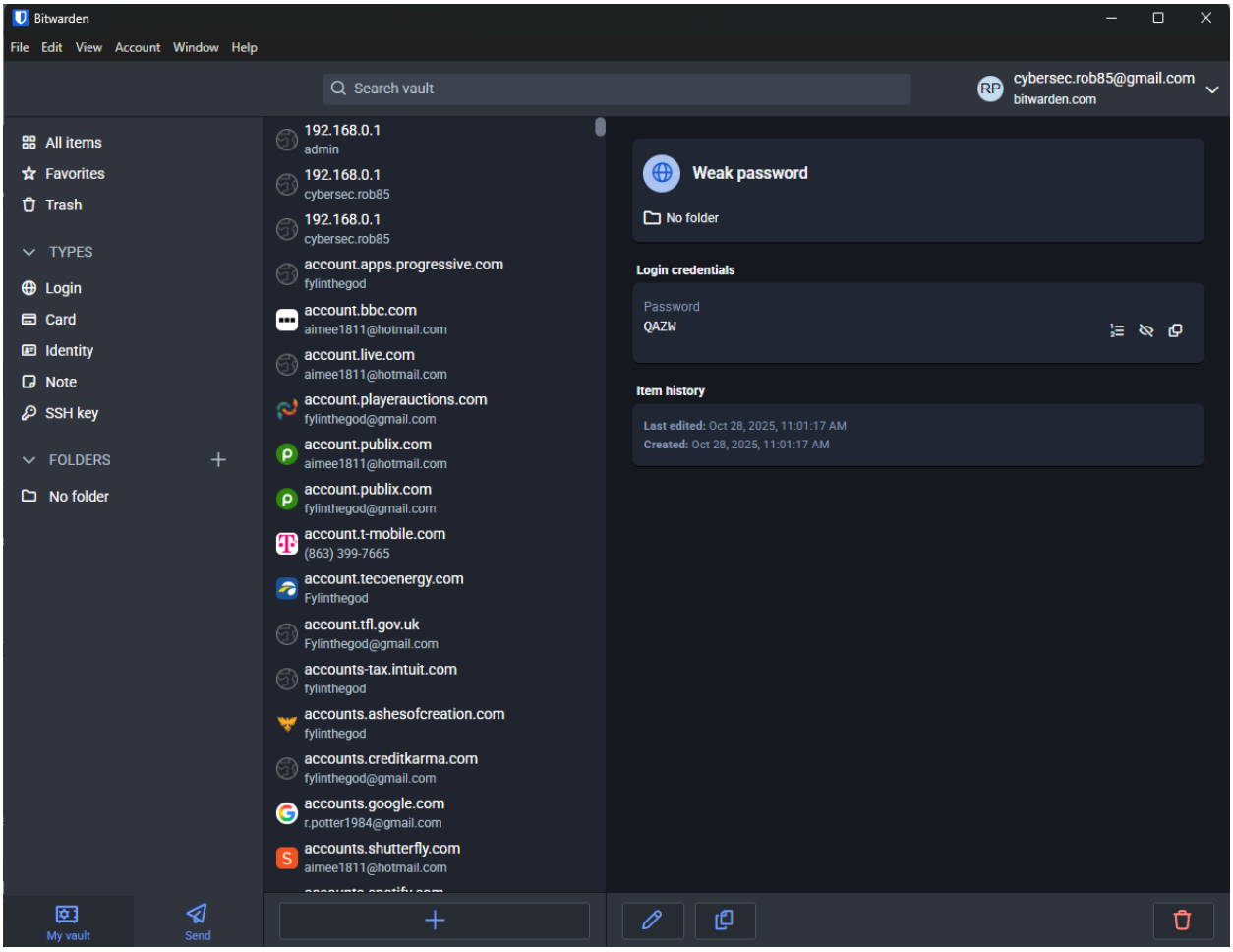
Deliverable: Take a screenshot of your Strong Password and include it in your lab write up. NOTE: Make sure that your password is visible (click the eyeball next to the password before taking the screenshot).



Task 3: Create a weak password using selected Password Manager

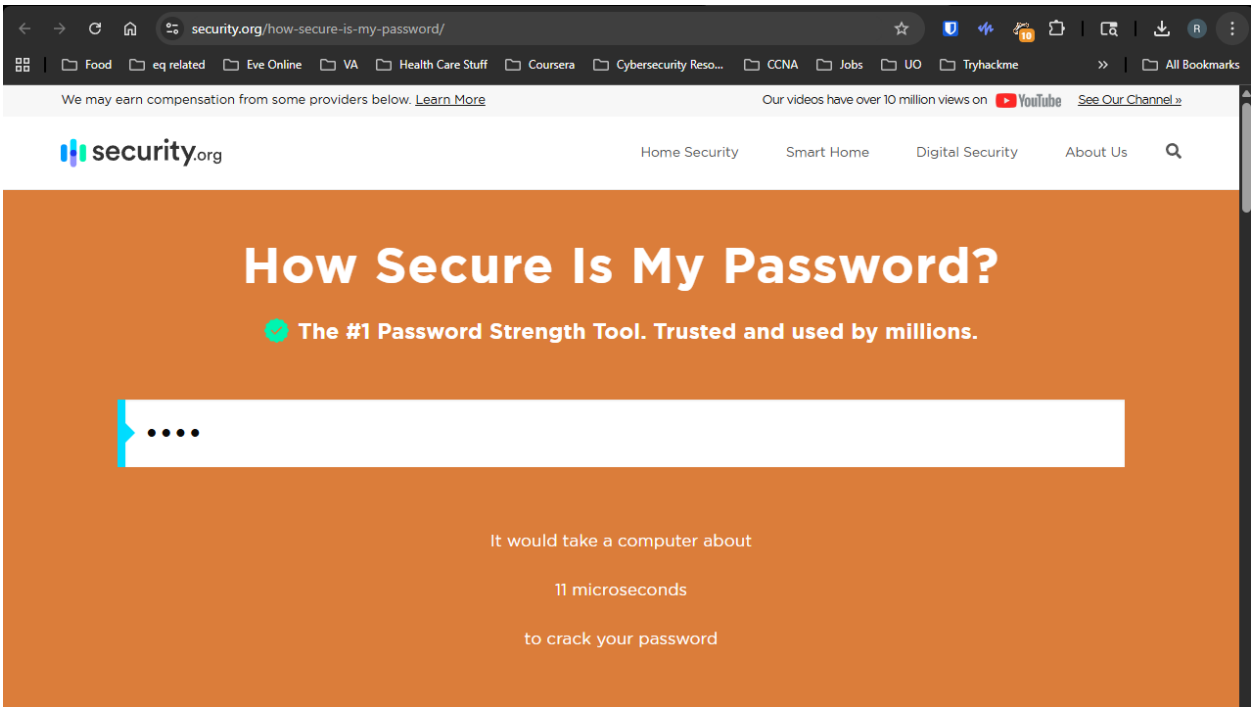
Deliverable: Take a screenshot of your Weak Password and include it in your lab write up. NOTE: Make sure that your password is visible (click the eyeball next to the password before taking the screenshot).

TIP: YOU SHOULD NEVER SHARE YOUR PASSWORDS! However, since these passwords were created for the purpose of this lab, it is OK this time.

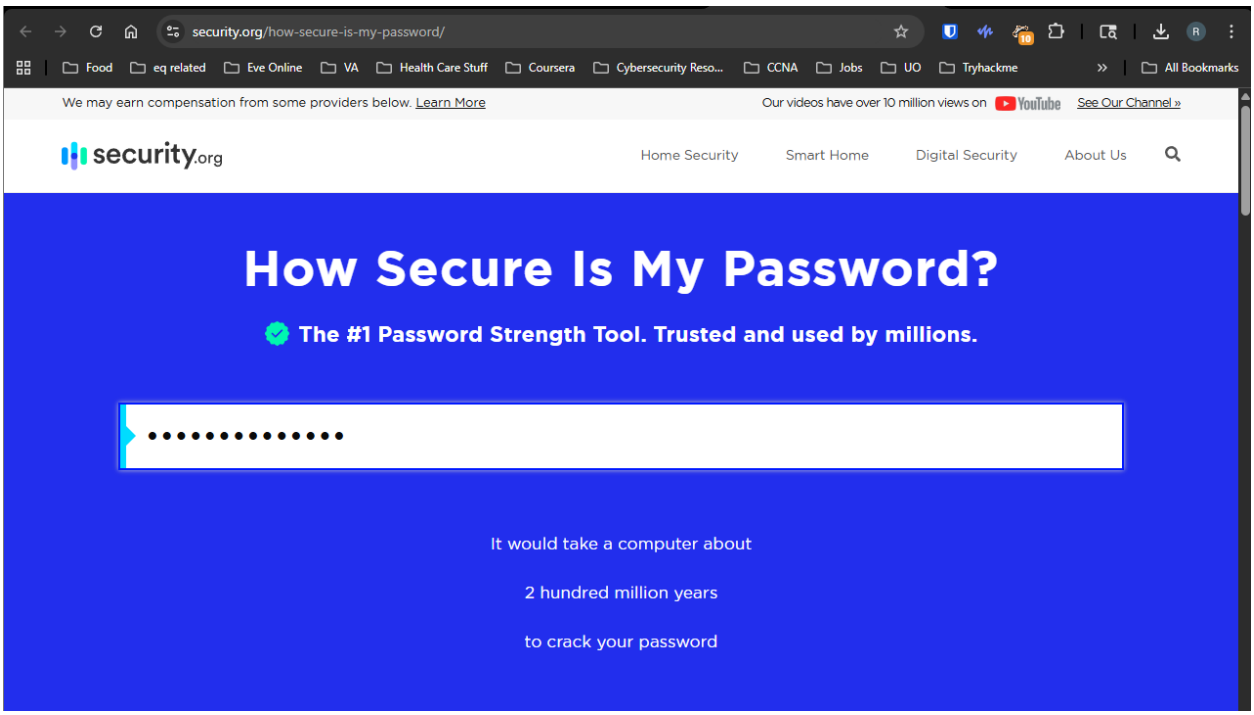


Task 4: Test your Password(s) strength

Deliverable: Include screenshots of the Strong Password and Weak Password results from the website in your lab write up.



Weak Password



Strong Password

Task 5: Create an MD5 hash of the strong password and the weak password

Deliverable: Include screenshots of MD5 output for the Strong Password and Weak Password in your lab write up.

Weak Password MD5

Your String	QAZW
MD5 Hash	a41906b7d472a04a519842f1420d6131 Copy
SHA1 Hash	8cb766b2aa34e8b9eb21fa7b3e3d417fdb350dbd Copy

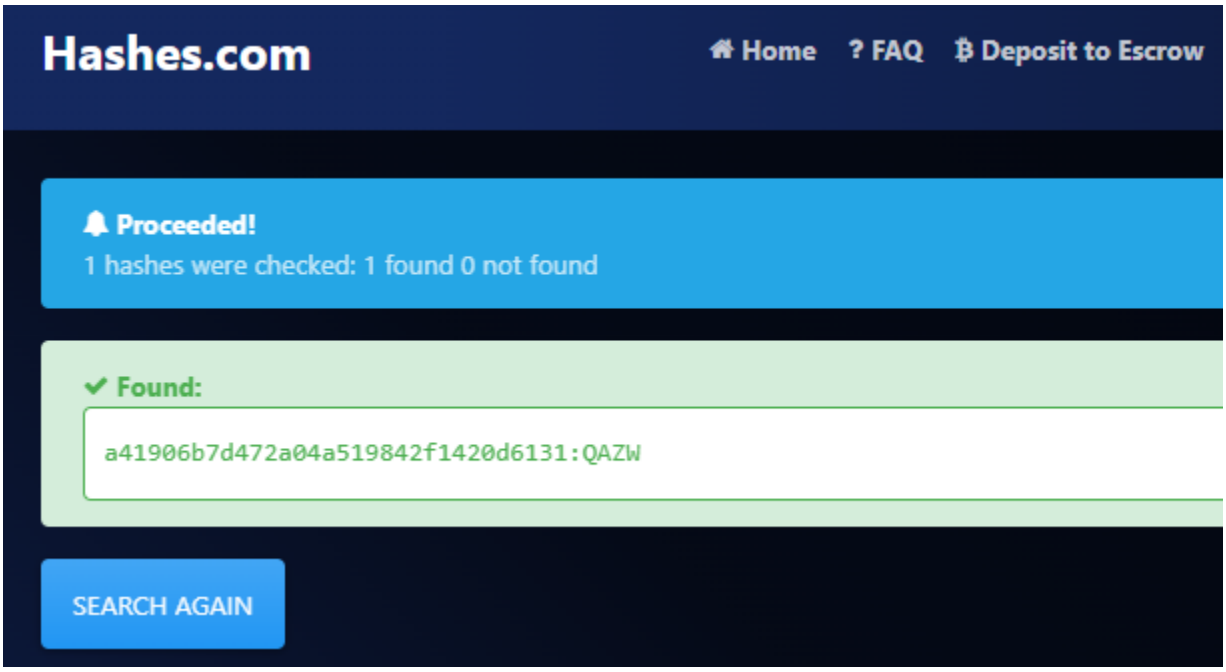
Strong password MD5

Your String	#5CtG3L8#qQw7ZuV
MD5 Hash	a567b830201579703055a848b920b812 Copy
SHA1 Hash	1c0710f29d801005b5b11fa90ad221951200f73e Copy

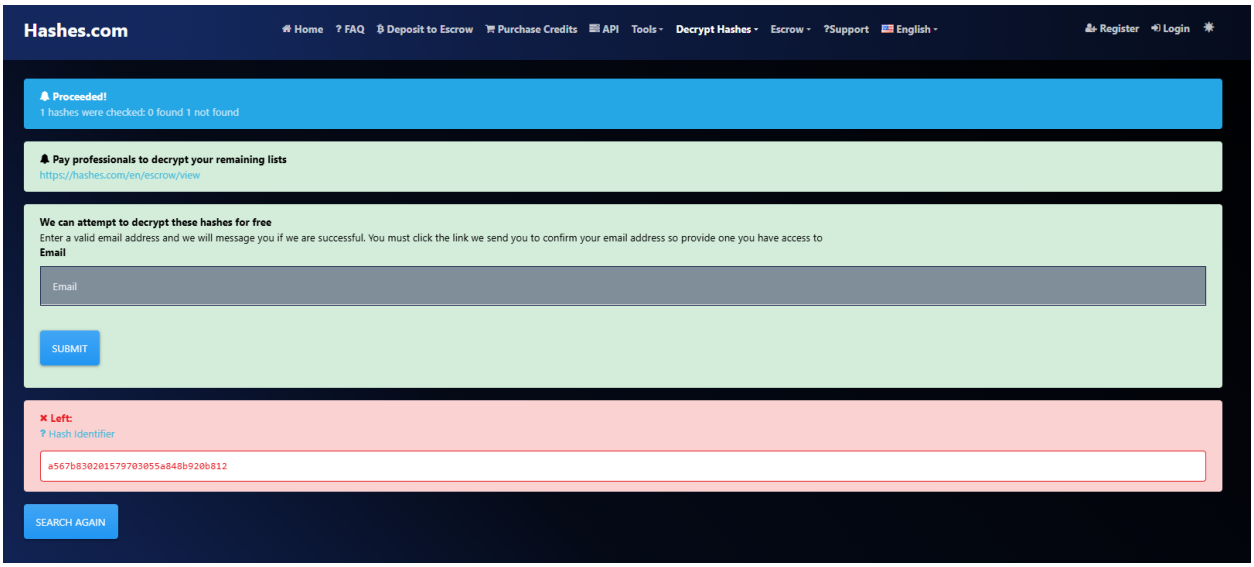
Task 6: Crack the MD5 hash of the secure password and the insecure password

Deliverable: Include screenshots of the MD5 cracking output for the Strong Password and Weak Password in your lab write up.

Weak Password

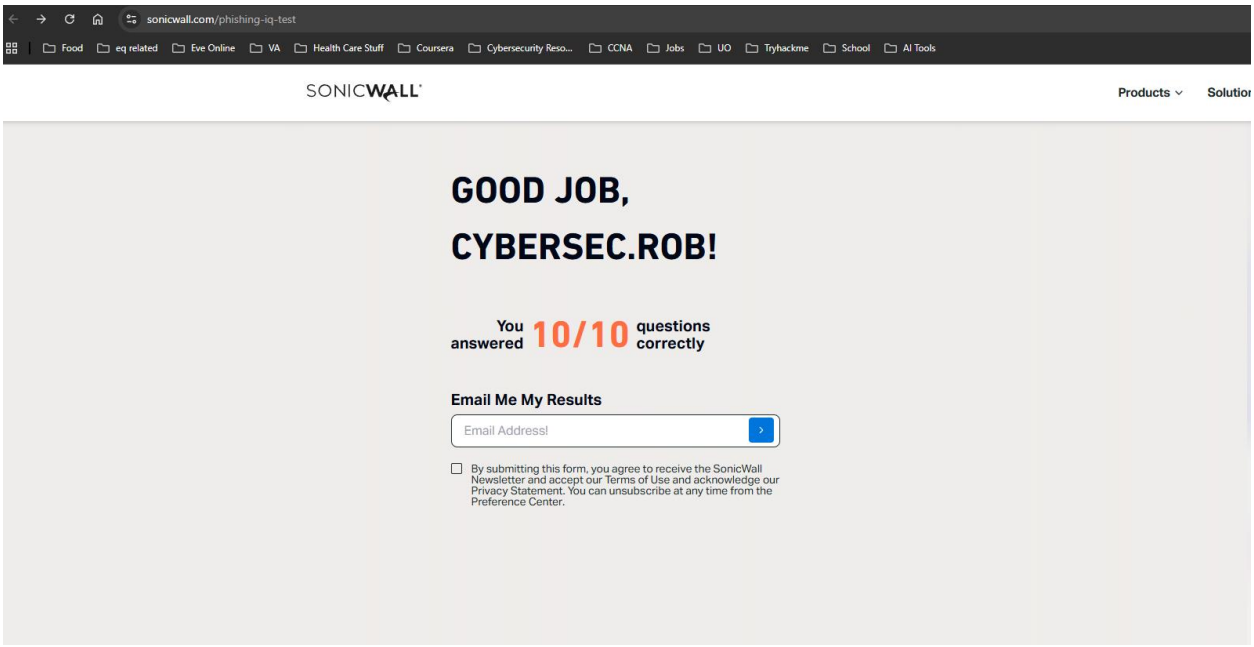


Strong password:



Task 7: Complete Dell Sonicwall Phishing Quiz

Deliverable: Include a screenshot of your quiz score in your lab write up.



Task 8 – Have I Been Pwned

Deliverable: None for Task 8

Lab Write up

Write a paragraph (2-3 sentences) for the three following questions related to the lab.

1. **What did you learn about the importance of a strong password?**

I learned that the difference in the number of characters and the use of special symbols can mean the difference between a password that can be brute forced in a matter of seconds to one that cannot reasonably be broken in years. This is why I started using a password manager a long time ago, both to make it easier to deal with logins and to also have unique passwords for every site I use so if one is compromised only that password is compromised.

2. **What could be done to improve the strength of the MD5 hash? Why is it effective?**

One way of improving the strength of the MD5 hash is to add a unique salt to either the beginning or the end of the input. By doing this, you will come out with a completely different MD5 hash than the original word's hash. This helps against sites like the one used in this lab to decode MD5 hashes.

3. **What is the importance of checking links in potentially fraudulent emails?**

It is important because attackers can make subtle changes to the address of a link even though the link text seems legitimate. Attackers also often use non-English characters that look the same as English characters, but they are not, and these will direct you to a site that can infect your computer with malware or try to harvest credentials. If you are not expecting an email from someone, it's always best to check with them to confirm its authenticity. Phishing remains one of the top reasons for security breaches.

Deliverable:

1. Gather the deliverables and lab write-up listed for each task in PDF Format
2. Name the file CTI2318-2025-Lab1-Firstname-Lastname.pdf where "Firstname" is your first name and "Lastname" is your last name
3. Upload to FSO in the appropriate area for Lab 1

Grading Rubric:

- ✓ **Submitted ALL write-up tasks: 10/10**
- ✓ **Included at least nine (9) screenshots: 45/45**
- ✓ **Phishing Quiz Results are Correct: 20/20**
- ✓ **References, paragraph for 3 questions w/ critical thinking + proofreading: 25/25**

References:

Question 2 information:
https://www.pingidentity.com/en/resources/blog/post/encryption-vs-hashing-vs-salting.html#:~:text=algorithm%20is%20used.-,What%20is%20Salting?,to%20duplicate%20or%20common%20passwords
.

Question 3 Research: https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams